ÉNS de Lyon — Agrégation
2018-2019

TD corps finis

Exercice 1 —[Algorithme de Cipolla (1907)] Soit $p \in \mathbb{P}\backslash\{2\}$. Soit $n \in \mathbb{F}_p$ qui est un carré. Soit $a \in \mathbb{F}_p$ tel que $a^2 - n$ n'est pas un carré. Soit $\sqrt{a^2-n} = \overline{X} \in \mathbb{F}_p[X]/(X^2-(a^2-n)) = \mathbb{F}_{p^2}$. Montrer que $(a+\sqrt{a^2-n})^{(p+1)/2} \in \mathbb{F}_p$ est une racine carrée de n.

Exercice 2 —[Peut donner lieu à un développement ...] Soit $\mathbb{F} = \mathbb{F}_q$ un corps fini de cardinal. Pour tout $Q \in \mathbb{F}[X_1, \ldots, X_n]$, on pose $S(Q) := \sum_{x \in \mathbb{F}^n} Q(x) \in \mathbb{F}$.

1. Pour a_1, ..., a_n, calculer $S(X_1^{a_1} \ldots X_n^{a_n})$.

2. Soient P_1, ..., P_r des polynômes de $\mathbb{F}[X_1, \ldots, X_n]$, de degrés d_1, ..., d_r. On note $Z := \{x \in \mathbb{F}^n | P_1(x) = \ldots = P_r(x) = 0\}$.

Si $P(x) := \prod_{i=1}^r (1 - P_i(x)^{q-1})$, exprimer $S(P)$ en fonction de $|Z|.1_{\mathbb{F}}$.

3. En déduire que si $d_1 + \ldots + d_r < n$, alors $|Z|$ est multiple de p (théorème de Chevalley-Warning).

4. En déduire que si les P_i sont des polynômes homogènes non constants (ou au moins si les P_i sont sans terme constant) et si $d_1 + \ldots + d_r < n$, alors le système $P_1(x) = \ldots = P_r(x) = 0$ a une solution non nulle dans $\mathbb{F}^n$.

5. Montrer l'application suivante (théorème de Erdös-Ginzburg-Ziv) : pour tout $n \geq 1$, pour tout $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$, il existe un sous-ensemble $I \subset \{1, ..., 2n-1\}$ de cardinal exactement n tel que $\sum_{i \in I} a_i \equiv 0[n]$.

Exercice 3 — Soit p un nombre premier impair. Montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1[8]$. (on pourra considérer ζ une racine primitive 8-ième de l'unité dans $\mathbb{F}_p$ et étudier $\zeta + \zeta^{-1}$.)

Exercice 4 — **1.** Soit $\mathbb{F}_q$ un corps fini, avec $p = \mathrm{car}(\mathbb{F}_q) \neq 2$. Montrer que $x \in \mathbb{F}_q^*$ est un carré si et seulement si $x^{q-1} = 1$.

2. En étudiant les diviseurs de $(n!)^2 + 1$, montrer qu'il existe une infinité de nombres premiers de la forme $4k+1$ ($k \in \mathbb{N}$).